SOPHOS

Security made simple.

VMware and vShield

An overview of setup

ESXi Host
vCenter and vSphere Client
vShield

Product version: 5.5

Document date: March 2014

Contents

1 About this guide....3
2 What you install....3
3 Install an ESXi host....4
4 Install vCenter....5
5 Install guest virtual machines....7
6 Install vShield Manager....8
7 Install vShield Endpoint....9
8 Appendix: Upgrade an ESXi host....10
9 Appendix: Move an ESXi host....11
10 Technical support....11
11 Legal notices....11

1 About this guide

This document tells you how to set up your VMware environment, your virtual machines and vShield security software.

After you complete these tasks, you will be ready to install Sophos Anti-Virus for VMware vShield to protect your virtual computers against malware and other threats.

This document also tells you how to upgrade or move VMware ESXi hosts on which you have already installed Sophos Anti-Virus (see the Appendices).

Notes

This guide is for version 5.5 of the VMware products. A guide for version 5.1 is available at *www.sophos.com/en-us/medialibrary/PDFs/documentation/savvv_1_bgeng.pdf*.

If you have already set up VMware and vShield, go straight to the *Sophos Anti-Virus for VMware vShield startup guide*.

Disclaimer

We have written this guide to help you configure your VMware environment to work well with Sophos Anti-Virus. We provide it in good faith and intend it to supplement VMware's own documentation or support advice. If you encounter issues, you should raise them with VMware as usual.

2 What you install

2.1 The VMware software

To set up and manage your virtual machines (VMs), you install:

- **ESXi host.** This is an application that runs on a server to enable it to host VMs.
- **vCenter.** This is a console that lets you manage multiple ESXi hosts and VMs centrally. You install it on a server.
- **vSphere Web Client.** This enables you to use vCenter remotely and conveniently. You install it on the vCenter Server but can then access it from a browser. (The Client is now installed as part of vCenter installation.)
- **Guest virtual machines.** These are the virtual computers you will be managing. You create them on the ESXi host.

Note: VMware software also includes a vSphere Client. This has the same function as the Web Client, but is installed on the computer from which you want to use vCenter.

2.2 vShield security software

To set up vShield security, you need:

- **vShield Manager.** This is a virtual appliance that you use to manage vShield Endpoint.
- **vShield Endpoint.** This passes requests for virus scanning to a third-party virtual appliance, such as Sophos Anti-Virus. This means that you do virus scanning centrally, rather than on each guest VM.

3 Install an ESXi host

3.1 What you need

You need a server that has:

- 64-bit processor.
- Two cores.
- Memory: 4 GB minimum, 8 GB recommended.
- Network speed: 1 Gbps minimum, 10 Gbps recommended.

You can find complete details of requirements at *www.vmware.com/resources/compatibility*.

3.2 Install the ESXi host

To set up an ESXi host, do as follows:

1. Go to *https://my.vmware.com/web/vmware/* and log in.
2. Find the downloads pages and download the ISO image for ESXi.

   The installers for VMware products are available from this page:
   https://my.vmware.com/web/vmware/info/slug/datacenter_cloud_infrastructure/vmware_vcloud_suite/5_5

   Tip: At the time of writing, the downloads page for ESXi is:
   https://my.vmware.com/web/vmware/details?downloadGroup=ESXI550&productId=351&rPId=4245
3. Burn the ISO image onto CD or DVD media.
4. Insert the ESXi CD in your server and restart it.
5. In the boot menu, select **ESXi Standard Installer**.
6. In the installer, you must:
   - Select the disk where you want to install ESXi.
   - Select a keyboard layout.
   - Enter a root password.

7. When installation is complete, the installer prompts you to restart.
8. After the restart, you see a screen where you can configure the system. Press F2.
9. Enter the root password.
10. In the **System Customization** page, select **Configure Management Network**. Now you configure:
    - **Network Adapters**. These provide the network connections for this host.
    - **IP Configuration**. Select **Set static IP address and network configuration** and enter the details.
    - **DNS Configuration**. Enter a **Primary DNS Server** address and a name for the host.
11. When prompted, confirm your changes and restart the host

4 Install vCenter

4.1 What you need

Before you install vCenter, ensure that your server meets these requirements:

Hardware

- 64-bit Intel/AMD processor.
- Two or more logical cores, each 2GHz.
- Memory: 12GB or more if you have a large inventory.
- Disk storage: 100GB.
- Network speed: 1 Gbps.

Software

- Minimum OS: Windows Server 2008 SP2.
- .NET 3.5 SP1 (vCenter Server installs this if necessary).
- MSI 4.5 (if you use the SQL Server bundled with the operating system).

Connectivity

The server:

- Should have a static IP address.
- Should not be a domain controller.
- Should be connected to Active Directory (if you are going to use it).

Database

Each vCenter must have a database.

If you have no more than 5 ESXi hosts or 50 VMs, you can use SQL Server 2008 Express. This comes with the operating system.

If you have more than 5 ESXi hosts or 50 VMs, check the requirements on the VMware website.

4.2 Download the vCenter installer

You must download the installer for vCenter Server and associated vCenter components.

1. Go to *https://my.vmware.com/web/vmware/* and log in.
2. Find the downloads pages and download the ISO or Zip file for **vCenter Server**.

   Tip: At the time of writing, the downloads page for vCenter Server is: *https://my.vmware.com/web/vmware/details?downloadGroup=VC550&productId=351&rPId=4245*
3. Extract the installer files to a temporary folder.

4.3 Run the vCenter installer

1. In the directory where you placed the installer files, double-click autorun.exe.
2. In the **VMware vSphere 5.5 installer**, under **VMware vCenter**, select **Simple Install.** Click **Install**.
3. A series of installation wizards run automatically to guide you through the installation of the components, as described below.

4.3.1 vCenter Single Sign On

In the installation wizard for **vCenter Single Sign On**, you must:

- Set a password for an administrator account.
- Enter a name for the vCenter Single Sign On site.
- Accept or change the HTTPS port to be used for vCenter sign on.
- Select the folder in which to install vCenter components.

Note: On Windows Server 2012, you are prompted to stop running the script that installs vCenter components. You must click **No**.

vCenter Single Sign On is installed. Next the installation wizard for **vSphere Web Client** runs automatically.

4.3.2 vSphere Web Client

The vSphere Web Client is installed non-interactively. You are not prompted to enter any settings.When installation is complete, the installation wizard for **vCenter Inventory Service** runs automatically.

4.3.3 vCenter Inventory Service

The vCenter Inventory Service is installed non-interactively. You are not prompted to enter any settings. When installation is complete, the installation wizard for **vCenter Server** runs automatically.

4.3.4 vCenter Server

In the installation wizard for **vCenter Server**, you must:

- Enter your license key.
- Specify a new or existing database for vCenter Server.
- Select the account with which you want vCenter to run.
- Accept or configure the ports that vCenter will use for communications.
- Select the amount of memory available for the vCenter inventory (depending on the number of hosts or VMs).

5 Install guest virtual machines

Now you use vSphere Web Client to access vCenter and set up your guest VMs.

Note: You will need Windows installation media (CD/DVD).

1. Go to the computer from which you want to access vCenter.
2. In the browser, enter: https://*vSphere_Web_Client_host_name_or_IP*:9443/vsphere-client/#

   Tip: In subsequent sessions, you can start the vSphere Web Client from the Windows Start menu, by selecting **Programs** > **VMware** > **VMware vSphere Web Client** > **vSphere Web Client**.
3. Click **Install this certificate and do not display any security warnings**, and click **Ignore**.
4. Right-click a host and select **New Virtual Machine**.
5. Select **Create a new virtual machine**. A wizard guides you through creating a virtual machine. You should:
   - Name your VM.
   - Specify a folder or datacenter where you want to create the VM.

- Specify the host (or other resource, for example cluster) for the VM to run in.
- Place the virtual machine files on the existing datastore.
- Accept the default setting for ESXi host compatibility.
- Select a Windows version that corresponds to the installation media that you own.
- Accept the default settings to finish the wizard.

6. Select the new virtual machine.
7. Place your Windows installation disk in the optical media drive of your local machine.
8. Click the **Connect/disconnect CD/DVD devices of the virtual machine** icon, and select the drive letter that corresponds to your DVD device.
9. Click the **Launch Virtual Machine Console** icon.
10. Select the console window for your new VM, and click the **Power On** icon.
11. Complete the Windows installation wizard.

6 Install vShield Manager

1. Go to *https://my.vmware.com/web/vmware/* and log in.
2. Click **Downloads**.
3. Under **Security Products**, go to the **VMware vCloud Networking and Security** page and follow the links until you reach the page with vShield Manager downloads.

   Tip: At the time of writing, the URL for this page is:
   https://my.vmware.com/web/vmware/details?downloadGroup=VCNS550_GA&productId=351&rPId=4245
4. Download the **.ova file** for vShield Manager.
5. In vCenter, select **File** > **Deploy OVF Template** and specify the .ova file you just downloaded.
6. The installer guides you through the installation. You must specify:

   - A name for the virtual machine (VM).
   - The host where you will install it.
   - The resource pool which will be used.
   - A datastore and network for the virtual network interface card in the vShield Manager to map to.
   - A disk format for the virtual disks.

   You might also need to configure the amount of memory used.
7. vCenter displays **Host Recommendations**. Select your host and click **Power On**.

vShield Manager is now displayed as a VM in vCenter.

6.1 Connect to vShield Manager and sync it with vCenter

1. To check that you can connect to vShield Manager, open a browser and enter the IP address you just set up.
2. Log in to vShield Manager as admin.
3. In the **Configuration** tab, in **vCenter Server**, click **Edit** and enter the vCenter information and credentials.

Now, on the same tab, register vShield Manager.

6.2 Register vShield Manager with the vSphere Client

1. On the **Configuration** tab, click **Register**.
2. Close the vSphere Client.

When you restart vSphere Client, you see tabs for vShield on the datacenter, cluster, host and port group objects.

You can also access the web user interface. At the home page, under **Solutions and Applications**, click the vShield icon.

7 Install vShield Endpoint

Installing vShield Endpoint involves:

- Installing the vShield Endpoint component.
- Installing the third-party security VM, in this case the Sophos security VM.
- Installing the vShield Endpoint Thin Agent on your guest VMs.

7.1 Install the vShield Endpoint component

1. In vCenter Server, select the homepage. Under **Solutions and Applications**, click the **vShield** icon.
2. In the **Host and Clusters** view, click the **DataCenters** node and then click the vShield host.
3. vShield Endpoint is shown as "Not installed". Click **Install**.

The vShield Endpoint component is installed without any input from you.

7.2 Install security VMs and vShield Endpoint Thin Agents

You are now ready to protect your VMs against threats. This involves installing:

- A Sophos security VM on each host.
- A vShield Endpoint Thin Agent on each guest VM.

For instructions, see the *Sophos Anti-Virus for VMware vShield startup guide*.

8 Appendix: Upgrade an ESXi host

If you upgrade an ESXi host that **already has a Sophos security VM installed**, you must take additional steps afterwards to ensure that the security VM still protects guest VMs.

You need to:

- Upgrade the host.
- Update vShield Endpoint.

Note: These instructions assume that you have already upgraded vCenter.

Upgrade the host

You can find advice and instructions in these VMware documents:

Installing or upgrading to ESXi 5.5 best practices (Knowledgebase article and video).

VMware vSphere 5.5 Documentation Center.

Tip: In the **Documentation Center**, look for *ESXi and vCenter Server 5.5 Documentation* > *vSphere Upgrade*.

After the upgrade, you will see that:

- The security VM and the guest VMs are still correctly listed in vSphere Client (see the **vShield** tab for the host).
- The security VM no longer detects threats.

You now need to update vShield Endpoint.

Update vShield Endpoint

1. Log in to vSphere Client (if you do not already have it open).
2. Select **Inventory** > **Hosts and Clusters**.
3. Select the host.
4. Click the **vShield** tab. The **General** tab displays each vShield component that is installed on the selected host and the available version.
5. Select **Update** next to vShield Endpoint.

6. Select the **vShield Endpoint** check box.
7. Click **Install.**

After you update vShield Endpoint, the security VM will detect threats and report to Enterprise Console again.

9 Appendix: Move an ESXi host

If you move an ESXi host **that already has a Sophos security VM installed** to a new vCenter (for example, to a vCenter that is a newer version), you need to remove and reinstall the Sophos security VM afterwards.

1. Follow the instructions in this VMware article:
   Moving an ESXi host from one vCenter Server to another.
   After the move, you will see that:
   - The security VM is no longer registered.
   - The security VM no longer detects threats.
2. In vSphere Client, find the Sophos security VM. Right-click it and select **Power Off**.
   Wait for the security VM to be powered off.
3. Right-click the security VM again and select **Delete from Disk**.
4. Run the Sophos Anti-Virus for VMware vShield installer again to reinstall the Sophos security VM.

10 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at *community.sophos.com/* and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at *www.sophos.com/en-us/support.aspx*.
- Download the product documentation at *www.sophos.com/en-us/support/documentation/*.
- Send an email to *support@sophos.com*, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

11 Legal notices

Copyright © 2014 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic,

mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.